Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 27 August 2003

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Washington Post reports that the nationwide average retail price of regular−grade gasoline went up to $1.75 a gallon on Monday, its highest level ever. (See item 1)
- The Associated Press reports that Banknorth Group said Monday that someone is sending their customers around New England e−mails to try to get their Social Security numbers, bank account numbers, and credit card numbers. (See item 6)
- CNET News reports that network hardware maker Netgear says a flaw in some of its router products could set off an "accidental" denial−of−service attack. (See item 22)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *August 26, Washington Post* — **Gasoline prices soar to highest point yet.** Gasoline prices around the country have risen to record levels. The nationwide average retail price of regular−grade gasoline went up to $1.75 a gallon on Monday, August 25, its highest level ever, according to the Energy Information Administration (EIA). The previous peak price of $1.73 per gallon was recorded on March 17. **Analysts attributed the rising prices to disruptions in production at a time inventories are already unusually low.** One major shock was the recent blackout in the Northeast and the Midwest, which temporarily shut down refineries in Ohio,

Michigan and Pennsylvania. In addition, a rupture in a gasoline pipeline that provides Phoenix, AZ, with about a third of its gasoline caused hundreds of service stations to close and prices to shoot up. **The disruptions came as supplies of oil have been abnormally low.** Over the past year, hurricanes on the gulf coast, the national strike in Venezuela and the war in Iraq have contributed to the low production levels, analysts said. As of August 15, total U.S. oil stocks, excluding the strategic petroleum reserves, were at 932.8 million barrels, down from 1.024 billion barrels at the same time last year, according to the EIA. Industry experts predict the high prices will not last long, as gasoline prices traditionally fall off steeply after Labor Day because fewer drivers are on the road and stringent summertime gas specifications designed to keep pollution down no longer apply, making it easier on suppliers.
Source: http://www.washingtonpost.com/wp−dyn/articles/A44771−2003Aug 25.html

2. *August 25, Dow Jones Business News* — **Dominion's Cove Point receives first LNG in 23 years. Dominion Resources announced on Monday, August 25, that its Cove Point LNG facility has received its first shipment of liquefied natural gas (LNG) in 23 years.** BP delivered 130,000 cubic meters of LNG from Trinidad and Tobago, a cargo that will ultimately be vaporized into approximately 2.9 billion cubic feet of natural gas, Dominion said. Cove Point LNG is a facility that transforms LNG back into natural gas. The technology allows the transporting of gas that is far from markets by transforming the fuel into a liquid that can be transported on tankers. As gas prices have risen in recent years, energy companies are turning to LNG as an additional source of natural gas.
Source: http://biz.yahoo.com/djus/030825/1634000845_1.html

3. *August 25, Reuters* — **FBI warns oil refineries and power plants. Refiners were operating with tightened security on Monday, August 25, after the FBI warned of a terrorist threat against petroleum and power plants in New York, NY, Los Angeles and San Francisco, CA.** The alert went out to FBI offices in those three cities late on Friday, August 22, said Special Agent John Iannarelli, a spokesman for FBI headquarters in Washington, D.C. "It's very vague and non−specific," Iannarelli said of the threat. "Post 9/11, we'd be remiss if we didn't pass on any information we have." The agency has issued similar warnings previously, but no attacks have occurred.
Source: http://biz.yahoo.com/rb/030825/energy_fbi_refineries_2.html

[Return to top]

Chemical Sector

4. *August 26, Indianapolis Star* — **Police probe chemical leak at farm co−op. The fertilizer tank leak that forced Monday morning's evacuation of more than two dozen families near Fountaintown was probably the work of an illegal drug maker**, an official said. "It's a theft for sure," said Ray Kerkhof, central crops manager for Ag One Co−op, which operates the facility where a 1,000−gallon tank of anhydrous ammonia was discovered to be leaking about 3:30 a.m. **Anhydrous ammonia is often used in the illegal production of methamphetamine, and thefts of the fertilizer, which can cause severe freeze−like burns and serious lung damage**, began occurring about five years ago in Central Indiana, Kerkhof said. Kerkhof said the co−op uses special caps that show whether anyone has disturbed the tank. While Hancock and Shelby county sheriff deputies roused more than two dozen families

downwind of the facility's tank farm, **about 23 specially trained Indianapolis Fire Department firefighters arrived to assist local firefighters**. IFD Capt. Gregg Harris said that when they arrived, a toxic cloud was hanging over the co−op's tank farm like a low−lying fog, and firefighters initially could not see which of the tanks was leaking. After setting up portable decontamination showers, two IFD firefighters in protective suits entered the fog to locate the leak.
Source: http://www.indystar.com/print/articles/1/068708−6561−009.htm l

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *August 26, Gulf Daily News (Bahrain)* — **Pakistan needs anti−money laundering law according to UN. According to speakers at a United Nations−organized seminar, Pakistan urgently needs a law against money laundering to fight the financial war on terror and endemic corruption. Pakistan is a key focus of U.S.−led efforts to trace and extinguish terrorist financing.** Extremist Islamic groups and some of Pakistan's 10,000 religious schools are suspected of channeling funds to terror networks like al Qaeda, often using an ancient system of money transfers through money changers and lenders outside of the banking system. The body tasked with tracing terrorist financing and probing suspicious transactions, the Federal Investigation Agency (FIA), urged authorities to be vigilant of donations made to religious schools, locally known as "madrassas." Some donations to religious schools are used for violent activities, FIA director general Mohib Asad told the seminar.
Source: http://www.gulf−daily−news.com/Articles.asp?Article=59995&Sn =BUSI

6. *August 26, Associated Press* — **Banknorth Group warns of scam fake website. Banknorth Group said on Monday, August 25, that someone is sending their customers around New England e−mails to try to get their Social Security numbers, bank account numbers, and credit card numbers.** Traditionally, such scams offer some benefit, such as increased amounts of credit or indicate that an account needs to be updated or validated. Some customers and non−customers received e−mails directing them to a false website, www.bank−north.us. The bank's real website is www.banknorth.com.
Source: http://www.thechamplainchannel.com/wnne/2433651/detail.html

7. *August 26, Associated Press* — **U.S. and Saudi Arabia to track terrorism financing. Agents from the FBI and the Internal Revenue Service are going to Saudi Arabia to establish a new joint U.S.−Saudi effort to track terrorist financing in the kingdom, a Treasury Department official said.** The program represents a ``renewed fervor on the part of the Saudis to get to the bottom of terrorism within their own peninsula," said David Aufhauser, the Treasury Department general counsel who heads the U.S. effort to combat terrorism financing. Previously, Saudi officials have responded to U.S. requests for information with questions

``about the adequacy of the evidence," Aufhauser said. Communications tended to have the tone of ``normal diplomatic discourse. It could be slow and frustrating. This unit is intended to be anything but that." The Saudi government has been cracking down on Islamic militants since the Riyadh suicide bombings last May. More than 200 suspects have been arrested and more than a dozen killed in a series of high−profile police raids, which also have uncovered computers and documents the task force intends to begin examining.
Source: http://www.nytimes.com/aponline/national/AP−US−Saudi−Terrorism.html?ex=1062924830&ei=1&en=333dde44d5a9e961

[Return to top]

Transportation Sector

Nothing to report.
[Return to top]

Postal and Shipping Sector

8. *August 25, Bloomberg* — **Legal challenge may slow Deutsche Post's U.S. expansion. Deutsche Post AG's expansion, in the U.S. ground and air parcel delivery market, may be slowed by a regulatory review sought by United Parcel Service Inc. and FedEx Corp. A U.S. judge today begins a hearing to determine whether Astar Air Cargo Inc., a Miami−based airline that flies for Deutsche Post's DHL unit, violates a law barring foreign control of a carrier.** UPS and FedEx lobbied for the Transportation Department hearing. **The judge's decision, due by December 1, may result in Deutsche Post having to change the way it does business in the U.S. A win by UPS and FedEx would slow or raise costs for Deutsche Post's advance in the U.S., the biggest delivery market, said Brian Clancy, principal at a freight−consulting firm in Virginia.** UPS controls 48 percent of the U.S. air−ground package and document delivery market, Clancy said. FedEx has 25 percent of the market based on revenue and Deutsche Post's DHL has 5 percent, he said. Other shares include the U.S. Postal Service with 14 percent and small competitors with a combined 8 percent, Clancy said.
Source: http://quote.bloomberg.com/apps/news?pid=10000085&sid=a6MiplR7XMxk&refer=europe

[Return to top]

Agriculture Sector

9. *August 26, High Plains Journal* — **Blue mold damage. Blue mold, a fungal disease that damages tobacco, has spread through a wet, gray summer and poses a threat to burley fields across Kentucky and into neighboring states. In every county of Kentucky, the disease either has been detected or the conditions are ripe for its growth, and the threat is the worst since 1996, when the disease caused about $200 million in damage, said Bill Nesmith, a University of Kentucky plant pathologist.** "We have a very threatening level of disease that is quite capable of causing economic damage on every farm in the state because we

do not know where those spores will blow tomorrow," Nesmith said. The disease reduces tobacco yields, and ultimately lowers income for growers. "There are very few counties that do not have active blue mold," Nesmith said. **The disease also has been spread into burley fields in North Carolina, Virginia, Tennessee, Ohio, and Indiana.** The disease is spread across long distances by airborne spores. The disease can occur sporadically. An infected tobacco patch might be near a second field that is spared entirely. "You can have massive losses, and it will vary from individual farm to individual farm," Nesmith said.
Source: http://www.hpj.com/testnewstable.cfm?type=story&sid=9641

10. *August 25, Canadian Press* — **Alberta to spend $15 million to boost mad cow testing. Alberta, Canada will spend $15 million to boost the number of cattle it tests annually for mad cow disease, Alberta Agriculture Minister Shirley McClellan said Monday. The province will increase the number of animals tested from 849 last year to up to 25,000 in the near future, she said.** Alberta, which produces 70 percent of Canada's beef, wants to help federal authorities meet a national goal of testing 65,000 head annually, she explained. **The money will be used to expand an existing Level 2 laboratory this year and to build a Level 3 bio−security lab in south Edmonton by 2005. It will also go towards hiring about 20 more veterinary pathologists, technicians, and meat inspectors to add to the current laboratory and food safety staff of about 100.** "These improvements will allow us to deal with testing surges should those occur and an appropriate turnaround time for all food safety." Cornelia Kreplin, director of Alberta's food safety division, said more staff working in an improved lab and with better methodology will prevent a backlog from developing in samples waiting for testing.
Source: http://www.canada.com/ottawa/story.asp?id=9BCC14BB−F290−4852−9E11−B4C07EB975FF

[Return to top]

Food Sector

11. *August 25, Chicago Tribune* — **Food industry safety.** Although the nation's food supply chain has come under scrutiny, experts question its ability to withstand attacks. Many of the largest food companies, they say, are working in a dangerous vacuum where vital studies are classified top secret and data required to help make informed judgments are kept under lock and key. "The food industry's biggest problem is the direction we need to take," said Dave Park, who heads a leading security consultancy. **"Most of the bigger firms have assessed the immediate risks themselves and understand some of the requirements. But it's the thousands of small firms that are most vulnerable." Worried that costs will be high, local companies have been reluctant to tackle a threat yet to be clarified by authorities, said Margaret Ann Daley, with the consulting and investigation arm of Pinkerton in Chicago.** Daley contends that most firms could radically improve security by taking a few basic measures at a cost of a few thousand dollars. **"The average food plant is less secure than many electronics plants," Daley said. "The electronics folks have been more worried about theft for years and as a result have become much more sophisticated when it comes to understanding who is working for them, perimeter security and access to plants."**
Source: http://www.centredaily.com/mld/centredaily/news/6615882.htm

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

12. *August 26, Reuters* — **China is premature in lifting SARS animal ban. The World Health Organization (WHO) called "premature" China's decision to lift a ban on the sale of 54 exotic animals deemed possible sources of the Severe Acute Respiratory Syndrome (SARS) virus.** China banned trade in the 54 species in May after declaring war on the disease which killed more than 800 people and infected more than 8,000. The clampdown emptied cages at bazaars in Guangdong, where SARS first appeared last November. The State Forestry Administration cleared the animals for commercial trade last week. **"From a public health perspective, it perhaps was a bit premature to lift the ban without having all the regulations in place to regulate the farm, trade, and consumption of wildlife," said Marie Cheng, WHO spokeswoman in Beijing. A team of Chinese and United Nations zoological disease specialists tested 100 different species of animals for SARS in the past week and found "some" tested positive, she said.** Cheng said further tests were needed to confirm whether the animals carried the virus, but added: "While these tests are still preliminary it is still suggestive." **The Forestry Bureau said the decision to remove the ban "did not mean these species do not carry viruses" but that they met conditions for commercial trade.** Source: http://www.enn.com/news/2003−08−26/s_7792.asp

13. *August 26, Pittsburg Post Gazette* — **Portable hospital prototype. The prototype for a federally funded disposable hospital has been erected in Monroeville, PA.** Covering more than 5,000 square feet, the floor, walls and some of the roof for the first Emergency Isolation and Treatment Shelter have been assembled during the past week. Today, government officials will tour the facility, which is the model for a portable structure that could be quickly assembled and then taken apart as needed to treat victims of bioterrorism or a natural disaster. **Polymer composite panels that weigh about 30 pounds each and measure 1 meter square are the shelter's building blocks. The idea is that kits containing enough panels to build a 500−bed hospital could be stored around the country, and then shipped and assembled where needed. The hospital can be built within 72 hours.** Because it's made of plastic, the one−story facility would be all−weather and could be easily cleaned. Disposal would also be possible. The structure being assembled in Monroeville will have room for 150 beds. While planners believe they will be able to build a shelter of that size in only 12 hours, it has taken four days to partially assemble the prototype. **The need for "surge capacity" was identified this month by the General Accounting Office as a challenge facing hospitals.** Source: http://www.post−gazette.com/pg/03238/215231.stm

14. *August 25, Canadian Press* — **Nursing home outbreak not SARS. The World Health Organization (WHO) has concluded that a respiratory disease that swept through a**

Vancouver, Canada nursing home this summer is not Severe Acute Respiratory Syndrome (SARS). Health officials in British Columbia said as much Friday. But today, the WHO endorsed that diagnosis, saying two lines of converging evidence allowed the organization to rule out severe acute respiratory syndrome. **In a statement, the WHO said the decision was made based on the fact that the patients involved did not manifest symptoms common to SARS, such as characteristic changes in lung X−rays. As well, genetic sequencing of a portion of a virus isolated from some of the 143 residents and staff of Kinsmen Place Lodge who fell ill did not match the SARS coronavirus, but appeared similar to a human coronavirus known as OC43.** "This virus, which is one of the causes of the common cold, has been associated with respiratory outbreaks in aged−care facilities in other countries," the WHO statement said.
Source: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1061849411874&call_pageid=968332188492&col=968705899037

15. *August 25, Reuters* — **World facing diabetes catastrophe. More than 300 million people worldwide are at risk of developing diabetes and the disease's economic impact in some hard−hit countries could be higher than that of the AIDS pandemic, diabetes experts warned on Monday.** In a report released at the International Diabetes Federation conference in France, experts estimate the annual healthcare costs of diabetes worldwide for people aged 20 to 79 are at least $153 billion. **According to the Diabetes Atlas report, total direct healthcare spending on the disease worldwide will be between $213 billion and $396 billion by 2025, if predictions are correct that the number of people with diabetes will rise to 333 million by 2025 from 194 million.** More than 75 percent of diabetes cases are expected to be in developing countries by 2025 because of rapid culture and social changes as well as increasing urbanization. This is expected to further burden healthcare systems already stretched by the AIDS pandemic.
Source: http://reuters.com/newsArticle.jhtml?type=healthNews&storyID =3332392

[Return to top]

Government Sector

16. *August 26, Associated Press* — **Three plead guilty in scheme that damaged Broward Port security. The president of a Port Everglades security company and two associates have pleaded guilty to hiring cruise ship guards without performing the required background checks**, the U.S. Attorney's Office announced. Edward Ebmeier, whose company provided security for 11 cruise lines operating at the port, pleaded guilty Monday in federal court to knowingly and willfully failing to comply with the requirements of the federal Terminal Security Plan. **The 58−year−old head of Port Services International Inc. also acknowledged lying to the U.S. Coast Guard by falsifying documents and state licenses**. He has been in jail since March 23 and faces up to 11 years behind bars and $500,000 in fines. Almeida Cetoute, 50, and Fritz Victor, 38, also pleaded guilty to a similar charge, authorities said. "The security of our ports and our cruise ships is no less important than the security of our airports and our passenger planes," U.S. Attorney Marcos Daniel Jimenez said. "This case is a demonstration of our commitment to ensure that our ports and our cruise ships are safe." **Investigators found 32 employees working with invalid or fraudulently acquired security documents, and also**

found Ebmeier hired workers without performing background checks.
Source: http://www.nbc6.net/news/2434362/detail.html

[Return to top]

Emergency Services Sector

17. *August 27, Associated Press* — **FEMA to survey backup systems. The 2003 blackout has prompted the nation's emergency management agency to survey the vulnerability of critical facilities such as water and sewage treatment plants, which failed along with the electricity**, the agency's head said yesterday. Mike Brown, director of the Federal Emergency Management Agency (FEMA), said in an interview with The Associated Press that he has initiated a national inventory of backup systems and vulnerabilities in the country's infrastructure to prevent future failures. The nation's worst blackout occurred August 14 after power failures darkened parts of Canada and eight states, from Ohio to New York. Water systems in Detroit and Cleveland were unable to handle the drop in power, and residents were asked to boil water while engineers made sure the system was free of contamination. "It is unacceptable to me that water treatment plants, for example, don't have backup power or that water treatment plants are susceptible to that kind of outage," Brown said, adding he was surprised to learn many Midwest water and sewage facilities could not maintain a clean water supply. "While I don't want to give a road map to terrorists of how to disrupt our economy and how to disrupt our lifestyle, I think we saw in Detroit and other places that that is a vulnerability we need to address." Brown, who was sworn in as head of FEMA and an undersecretary of the Department of Homeland Security in April, did not say how long it would take to complete the massive fact−finding effort, which will look at other possible weaknesses besides water treatment. He said **FEMA also was conducting an internal review to determine how many of its own emergency response facilities lack backup power**.
Source: http://www.newsday.com/news/nationworld/nation/ny−usblac263429199aug26,0,1055563.story?coll=ny−nationalnews−headlines

18. *August 27, Stateline.org* — **Kansas City develops Internet−based security system. A coalition of city governments is preparing to launch an Internet−based homeland security initiative in Kansas City that is meant to help emergency workers better respond to terrorism or natural disasters**. The computer system, operated by the Mid−America Regional Council (MARC) of governments and created by a Kansas−based software company, is to connect more than 100 government agencies across eight counties and two states in the Kansas City metropolitan area. **The system is expected to launch in early 2004 and will allow emergency personnel from different cities in Kansas and Missouri to share information and coordinate their efforts during a disaster**. Officials believe Kansas City's Metropolitan Emergency Information System (MEIS) to be the first of its kind in the United States.
Source: http://www.govtech.net/news/news.php?id=2003.08.26−65629

19. *August 26, NBC5.com* — **State police: worm virus knocked out dispatch system. Illinois State Police officials are trying to determine how a computer worm that struck two weeks ago knocked out a dispatching system that helps protect troopers and required disinfection of all 3,500 state police computers**. Officials, surprised by the worm's success, are reconsidering their decision to rely on individual employees −− some of whom may have

been absent −− to install the antivirus "patches" necessary to protect the state police system. **The computer−aided dispatch program, CAD, is not connected to the Internet, and state police say they don't know how the Web−based worm reached the program**. The infected dispatching system links to state police criminal records files. If the worm had reached them, it could have crippled the agency's ability to share information with other police departments or to check drivers' criminal records during traffic stops. Master Sgt. Rick Hector, the agency's spokesman, acknowledged the loss of some of the dispatch system for several hours, but said public safety and service was never affected. Hector said infection of criminal record databases was "in theory" possible, though he stressed it didn't happen. But the incident raises questions about the vulnerability of state police computer systems.
Source: http://www.nbc5.com/news/2433699/detail.html?z=dp&dpswid=2265994&dppid=65192

[Return to top]

Information and Telecommunications Sector

20. *August 26, Government Computer News* — **Stenbit urges IT crews to be forward−thinking. John Stenbit, assistant secretary of the Department of Defense (DoD) for networks and information integration is working toward an IT transformation at the DoD, including a shift to IPv6 by 2008, with the goal of achieving a network−centric approach**. Data, applications and communications must be interwoven to result in the right information to warfighters, Stenbit said. Some elements, such as the launching of communications satellites to extend DoD's Global Information Grid to wireless devices, have been sharply questioned by congressional appropriators, who have called for cuts in Defense's IT funding requests. As a result, Stenbit told reporters that he and other officials would be more careful in delineating requests for future tactical systems as compared to funds for more mundane administrative systems. **Another goal is to create data once and then tag it with metadata so that it can be found and used for multiple applications**.
Source: http://www.gcn.com/vol1_no1/daily−updates/23291−1.html

21. *August 26, Federal Computer Week* — **Syracuse police go wireless.** The Syracuse, NY, Police Department is moving toward a wireless infrastructure so officers and civilian employees have easier and quicker access to information. **Syracuse police began upgrading their laptops with wireless access cards and installed access points in certain areas about a year ago. The department is testing wireless thin clients and planning to provide better wireless access for officers in patrol cruisers**. Patrick Phelps, the department's information technology specialist, said wireless technology makes investigators more efficient. Previously, investigators would interview witnesses in one room, walk to another to type their statements, print them out and then review them with witnesses to ensure accuracy. If the statements weren't correct, the investigators had to retype statements before the witnesses could sign it. Now investigators take a laptop into the interview room to type statements or access other information, saving time and effort, he said. **The city's long−term goal is to deploy high−bandwidth hot spots near its main station and substations** so officers can better access the department's intranet for daily bulletins and other information.
Source: http://fcw.com/geb/articles/2003/0825/web−syr−08−26−03.asp

22. *August 26, CNET News* — **Netgear flaw triggers 'accidental' attack. Network hardware maker Netgear says a flaw in some of its router products could set off an "accidental" denial−of−service attack**. The problem occurred because of a flawed implementation of the Network Time Protocol (NTP), which is a method commonly used by network devices to contact special "time" servers that pass on the correct time and date. The flawed routers work fine until one of their periodic requests for the correct time goes unanswered. If for whatever reason the time server is unavailable, the flawed router will continue sending requests until it is answered. **Earlier this year, the University of Wisconsin's NTP server was the victim of a huge denial−of−service attack. The university claims it was receiving 250,000 requests per second**, which equated to hundreds of megabits per second. The attack was not planned or malicious, but caused by hundreds of thousands of low−cost Netgear routers repeatedly requesting the latest time, causing the university's NTP server to fail. **A patch is available on the Netgear website**: http://kbserver.netgear.com/kb_web_files/n101176.asp.
Source: http://news.com.com/2100−1002_3−5068035.html?tag=fd_top

Internet Alert Dashboard

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_SOBIG.F** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 80 (www), 1434 (ms−sql−m), 137 (netbios−ns), 1433 (ms−sql−s), 445 (microsoft−ds), 139 (netbios−ssn), 1243 (BackDoorG), 27374 (SubSeven), 17300 (Kuang2TheVirus) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

23. *August 26, New York Times* — **Blackout shows Canada−U.S. links in security vulnerability.** The power failure on Thursday, August 14, was a stunning reminder to Canadian officials of lessons they learned after September 11, 2001, on the risks for Canada from a terrorist attack on the United States. **In the last two years both countries have taken a host of measures to secure the common 5,500−mile border and protect vital power and pipelines, railways, roads and bridges that link them.** According to official figures, 60 percent of the $1.4 billion of daily trade between the two countries is funneled through four bridges and one tunnel that

run through the Great Lakes region; those crossings also carry gas pipelines and electrical and telecommunications lines. Canada is allocating much more of its budget to fight terrorism, and the two countries cooperate on many efforts to bolster security. Law enforcements operations have become closer, including the sharing of customs agents and coordinating anti−smuggling activities across the border with new computer software and radio systems that share information instantaneously.
Source: http://www.nytimes.com/2003/08/26/international/americas/26C ANA.html

24. *August 26, Santa Cruz Sentinel (CA)* — **Unexpolded grenade found at dump. Workers at the Santa Cruz, CA, city dump found an unexploded hand grenade on Monday, August 25. City police were called as was a bomb expert, Sgt. Amy Christey with the county Sheriff's Office, who decided to summon an explosives team from Fort Hunter Liggett in Monterey County, CA, to take care of the grenade.** The Fort Hunter Liggett crew drove to the dump, picked up the grenade, and transported it back to base with them. Police and workers say the situation could have been disastrous had the grenade not been found when and where it was. Crews at the landfill use heavy trucks and Bobcats, sort of mini−bulldozers, that could have set off the ordnance.
Source: http://www.santacruzsentinel.com/archive/2003/August/26/loca l/stories/04local.htm

[Return to top]

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer